

Before Making the Leap, Check Cloud Security - and Check Your Own

By Ed Moyle

TechNewsWorld

Just because using a cloud service means your important enterprise data will reside on an off-premise site does not make the system inherently less secure than keeping it in-house. Before making the jump to the cloud, though, some research should be done in terms of security -- both the service provider's and your own.

Most of us are probably familiar with safe deposit boxes -- you know, the secure storage areas that banks and post offices provide to keep things like jewelry and important documents secure. Even if you've never rented one yourself, chances are you're probably familiar with the concept: a safe place where you can put important and one-of-a-kind items so that they'll be protected should the unexpected occur in your home (like a fire, theft or flood).

Ask yourself this: Is a safe deposit box insecure because it's located and accessed from outside your home? In other words, in thinking about the security of the safe deposit box, would you conclude, "I don't trust the bank vault because I don't manage and control it myself?" Probably not, right? In fact, most likely we would conclude the opposite -- that the box is more secure because it's outside the home. Bank vaults are harder to steal from than our homes.

When it comes to everyday life, we realize intuitively that a location is not de facto more secure just by virtue of the fact that we're the one making decisions about how to secure it. It would be ridiculous, for example, if a friend told us that they prefer to keep important papers in a disorganized pile on their bedroom floor because it's inside their home -- and therefore more secure.

So what's my point? A lot of us in the security industry have been getting a bit nervous about decisions that our organizations are making in and around cloud computing. The cloud is a juggernaut in IT right now, and it's buzzing throughout all our organizations. Because it's such a hot topic, a lot of information security and compliance professionals are justifiably concerned about the security impacts of storing critical data in the cloud. Think about it: We're relocating large portions of our critical data to locations outside the firm's technical boundaries -- what does that mean from a security perspective?

There's a lot of concern, and rightly so, because storing or accessing data inappropriately can have a legal, financial or other catastrophic impact. Our first reaction is to cling to old ways of doing things and resist the move to the cloud, because that's what we know and are familiar with. However, it's important for us to remember during all this that just because we control something ourselves, that doesn't always mean it's better.

What Do You Have Today?

Now don't get me wrong -- I'm absolutely not saying that every service provider is the digital equivalent of a safe deposit box. Some are, some aren't. In point of fact, some service providers are much worse from a security perspective than what we can do ourselves (and some are much better.) However, the point is that the security decisions we make aren't (or shouldn't be) just based on where the data is stored; it's much more complicated than that.

If we have the metaphorical equivalent of the disorganized pile of papers internally (i.e., a mishmash of insecure storage, broken access controls, and lax/unmonitored processes for data handling), we may actually be better off from a security perspective making a transition to something hosted externally (depending, of course, on what the vendor provides). On the other hand, if we run a pretty tight ship, we might put ourselves in a worse position by making a change.

Many of our organizations are like our friend with the disorganized pile; some other lucky few have the digital equivalent of a fire box or safe internally. However, most of us are the opposite, with very little idea where our data goes, where critical data is stored, who accesses it, why it's accessed or from where.

In order to make an informed decision, we have to know two things: the security profile of what we're doing today and the profile of what the vendor in question does. If we're in a "papers on the floor" kind of organization and we're looking at a "safe deposit box" cloud service provider, we might choose to do one thing. If we're a shop with robust security controls and we're considering a "fly by night" vendor, maybe we might make a different decision. The point is, knowing those two data points, we can methodically and systematically compare in-sourced to outsourced and make a decision based on facts rather than based on speculation or (worse yet) industry hype.

So how do we get to that? First, start by mapping out what data you currently have, what processes govern how it's accessed, and the controls that you have in place to protect that data. Leverage any formal risk assessment that you may have done in the past (for example, to meet regulatory mandates like HIPAA, PCI or FISMA). If you haven't done a formal risk assessment of your environment, now's the time to do one. It's not as difficult as it used to be with new standard approaches and automated tools. On the standards side, leverage methodologies like ISO 31000:2009 or OCTAVE; on the tools side, look to automated risk-assessment products like White Cyber Knight's WCK-Lancelot or Modulo Risk Manager to automate the process.

You don't want to go to tremendous levels of detail here -- the point is just to get to enough of an understanding of the risk in our environment to be able to make a comparison against the vendor(s) in question. Also, make sure you map out in detail potential threat scenarios (for example, a threat matrix) that includes potential threats like inappropriate access, vectors (pathways) for access, accessibility issues (e.g., disasters), and so forth.

What Does the Vendor Have?

Next, we have to figure out what the vendor does or doesn't do to protect the data entrusted to them. Ideally, we want to be get enough detail about a vendor to be able to directly compare the risk assessment we have of our environment to the vendor. The challenge, however, is that the vendor may not be able (or willing) to share with us the details of the security controls that they have in place. For example, a vendor may not have confidence enough in their security controls to tell us candidly what they are; they may have a "security through obscurity" belief that not telling us how they protect data provides security value. Whatever the case may be, expect there to be a threshold -- a level of detail that you can't get beyond because of resistance from vendor personnel.

So if we can't get to a complete level of detail for a particular (or any) vendor, what then are we to do? First, put together a mirror of the threat matrix that you did for your own environment -- this lets you understand what potential exposure scenarios there are depending on the decision you make. Second, gather what data you can from the vendor about controls and risks; if there's been an industry-accepted evaluation done (such as a BITS shared assessment or ISO 27001 certification), these can be a good baseline since they both outline minimum baseline controls. If there is no accepted certification, consider vetting the vendor yourself -- either by going there and evaluating their security in person or a paper-based exercise such as a questionnaire. Remember, you don't need to go to a tremendous level of detail -- you only need to get enough that you can make an informed decision based on the facts.

With a level of detail about both your own internal environment as well as a fairly thorough understanding of the vendor environment, you should have enough data to do a methodical, repeatable and objective analysis of both environments. Sometimes going with the vendor is a better security decision, sometimes keeping it in house is. Sometimes your business partners will elect to trump security and go with the less-secure option for reasons not involving protection of the data. However, when based on solid analysis, at least the decision is an informed one.